UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

UNITED STATES OF AMERICA, Plaintiff, vs. NICHOLAS BICKLE, Defendant.	Case No. 2:10-cr-00565-RLH-PAL **REPORT OF FINDINGS AND RECOMMENDATION** (Mtn to Suppress - Dkt. #92)

This matter is before the court on Defendant Nicholas Bickle's ("Bickle") Motion to Suppress Evidence (Dkt. #92) filed on March 9, 2011, which was referred to the undersigned for a report of findings and recommendation pursuant to 28 U.S.C. § 636(b)(1)(B) and LR IB 1-4. The court has considered the Motion, the government's Response (Dkt. #105) filed March 25, 2011, Bickle's Reply (Dkt. #110) filed April 4, 2011, the representations and arguments of counsel at a hearing conducted May 13, 2011, and evidence adduced at an evidentiary hearing conducted June 10, 2011.

BACKGROUND

Bickle was charged, along with two co-Defendants, Andrew Kaufman and Richard Paul, in a single-count Complaint (Dkt. #2) on October 29, 2010, with conspiracy in violation of 18 U.S.C. § 371. An Indictment (Dkt. #21) and a Superseding Indictment (Dkt. #49) were returned on November 23, 2010, and December 14, 2010, respectively. The Superseding Indictment charged all the Defendants with conspiracy and thirteen various firearms offenses.

In the current motion, Bickle seeks to suppress emails obtained by the government pursuant to a search warrant served on Microsoft for the contents of Bickle's Hotmail account. Before the search warrant was obtained, Assistant United States Attorney ("AUSA") Drew Smith sent a preservation

letter to Microsoft concerning Bickle's Hotmail email account on December 1, 2010. On January 11, 2011, the government applied for a search warrant directed to Microsoft which was supported by an affidavit of probable cause submitted by Special Agent Eric Fox of the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"). The search warrant was issued by United States Magistrate Judge George W. Foley the same day. On February 7, 2011, defense counsel received a disk in discovery from the government that contained the emails provided by Microsoft in response to the search warrant. The government applied for and was granted an order unsealing Agent Fox's affidavit in support of the search warrant, and a copy was provided to counsel for Bickle. A copy of Special Agent Fox's affidavit is attached as Exhibit "A" to the motion.

DISCUSSION

I. The Parties' Positions.

A. Bickle's Motion to Suppress (Dkt. #92).

Bickle asserts that the search warrant was based on mere speculation, conjecture, and possibilities that failed to establish probable cause and that it was overbroad as to time and scope. Additionally, he claims that the affidavit contains materially misleading statements that entitle him to a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978).

Bickle acknowledges that in deciding the motion to suppress, this court's review is limited to determining whether substantial evidence supported its issuance and that the court does not conduct a *de novo* review. However, he claims Agent Fox's affidavit lacked substantial evidence and contained only "flimsy inferences" to support the agent's belief that relevant evidence might be found in Bickle's Hotmail account. For example, the assertion that Bickle used his Hotmail account to contact people who "could potentially be witnesses or targets of the government's investigation" is insufficient to establish probable cause to search the account for evidence of firearms trafficking crimes. Bickle also contends the affidavit does not establish probable cause to search for travel information because it only states that Bickle traveled during the period during which the conspiracy allegedly occurred, used his email to confirm those travel reservations, and that firearms were distributed in various states.

Additionally, the affidavit's reference to an email from Bickle to Matthew Klier advising Klier that the ATF may approach him and noting that other people have retained counsel does not establish

probable cause to believe Bickle's email account would contain evidence of witness tampering. Bickle also maintains the affidavit lacked probable cause to search his Hotmail account for his communications with Microsoft technical support or to obtain records of his online subscription services. For all of these reasons, Bickle argues the affidavit supporting the search warrant failed to make a particularized showing of probable cause to believe that crimes had occurred and that evidence of those crimes would be found in his email account.

Second, Bickle argues the emails seized should be suppressed because the search warrant was overly broad in both time and scope. Bickle asserts he had a reasonable expectation of privacy in his email account, as evidenced by the fact that the account was password protected and contained communications with his attorneys and therapist. Relying on *United States v. Washington*, 797 F.2d 1461, 1473 (9th Cir. 1986), he maintains the warrant is "patently overbroad" because it permits seizure of information about people associating with him. Additionally, Bickle claims the warrant is overbroad because it contains no temporal limitation for seizing information from the email account despite the fact that the government alleges the conspiracy and arms transactions occurred between March 30, 2009, and November 4, 2010. The warrant should have been restricted to production of responsive emails created, sent or received during the period of alleged criminal conduct.

Bickle argues that the warrant is so overbroad that it amounts to a general warrant that authorized a rummaging through his personal belongings which is prohibited by the Fourth Amendment. The search warrant was not limited to the charged offenses and instead sought to seize all communications Bickle made or received via his email account. The warrant also failed to contain necessary language identifying emails and files constituting attorney-client communications or attorney work product in violation of 42 U.S.C. § 2000aa-11. Although the affidavit assured the court that a filter agent would be assigned to review and remove any potentially privileged materials recovered from the warrant, this was not done. As a result, Bickle asserts investigating officers and prosecutors involved in this case obtained and read confidential attorney-client communications directly related to his defense.

Bickle also argues that the warrant's authorization to seize address books, contact, buddy lists, and technical support materials rendered it overbroad because there was no basis for probable cause to

obtain these records. The address books or contact information can only be used to obtain evidence of association which is prohibited, and the affidavit does not contain any discussion why records regarding communications between Bickle and Microsoft's technical support services were being sought.

Finally, Bickle asserts he is entitled to a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), because there are false or misleading statements in the affidavit which were material to a finding of probable cause. Specifically, Bickle contends the affidavit intentionally misled the court by suggesting that he and his co-Defendants sold guns to an undercover ATF officer, when the government has no evidence that Bickle ever sold guns to an undercover ATF officer. Bickle also claims that the affidavit improperly misled the court to draw the inference that Bickle tampered with witnesses by using his email account when the government has no evidence to support this inference. The affidavit refers to emails Bickle is alleged to have sent to Matt Klier telling Klier that he may be contacted by ATF and that "some guys have opted [for] lawyers and have ben [sic] left alone. I hope you are doing well." Nothing in this email is a violation of law, but is a "red herring" intended to mislead the court into believing Bickle was tampering with witnesses. Additionally, Bickle claims the government intentionally commingled unrelated events to mislead the court about wire transfers Klier received from Bickle. The $800.00 wire transfer referred to in paragraph 25 of the affidavit related to paying Klier for repairing Bickle's motorcycle, about which the government knew. However, the way the affidavit is written suggests that wire transfers were made which were related to the sale of firearms to an undercover agent by co-Defendant Richard Paul. The affidavit also refers to an email exchanged with Jason Cole which Bickle contends is another "red herring" intended to create the impression that Bickle used his email and texts as a tool to sell guns to Cole when the government has no evidence to support this baseless implication.

B. The government's Response (Dkt. #105)

The government opposes the motion arguing that under the totality of the circumstances, Judge Foley had a substantial basis for concluding that probable cause existed to seize the contents of Bickle's email account. The affidavit supporting the search warrant relates that ATF learned that Bickle used the email account polarbickle@hotmail.com and cooperating Defendants indicated Bickle used this account as his primary means of contacting people while deployed in Iraq until March 2009. This

March 2009 time frame is when the government asserts Bickle was smuggling the large majority of firearms at issue in this case into the country. Co-defendant and co-conspirator Richard Paul was in email contact with Bickle at this time. These facts establish a fair probability that evidence of Bickle's crime would be present in his email account.

Additionally, the affidavit relates that ATF learned Bickle used his email address to contact potential witnesses and targets in this case. Potential witness Jason Cole had cooperated with ATF, but after Bickle wrote a message to him, he stopped cooperating. On another occasion, Bickle sent an email to potential witness Matt Klier. The content of the email was related in the affidavit which was sent one day after ATF interviewed Klier's employer, Global Studies Group, about the underlying firearms trafficking scheme. Thus, the government maintains that under the totality of these circumstances, there was a sufficient basis for the issuing judge to determine Bickle was attempting to obstruct justice or engage in witness tampering and that evidence of these offenses would be found in Bickle's email account. The affidavit referenced discussions about wire transfers which referred to motorcycles or motorcycle parts because the government had information from co-Defendant Paul that Bickle told Paul to explain wire transfers derived from firearm sales as payments for a motorcycle. The affidavit appropriately sought information about Bickle's travel because ATF had information that Bickle traveled extensively during 2009 and 2010 and that firearms were distributed in at least three states as part of the conspiracy involved in this case. The affidavit indicated that ATF knew that Bickle used the Hotmail account address for Southwest Airlines as of November 2010 and received a text message during the period of the conspiracy stating that his hotel confirmation had been sent to his email account.

More importantly, the affidavit related that ATF learned Bickle used and continued to use the Hotmail account to communicate with individuals he was supplying with illegally imported firearms. Bickle's use of text messages, and the capacity of his email box, coupled with the preservation letter ATF sent to Microsoft made it likely that any messages sent to Bickle would still be in the Hotmail account.

The government disputes that the warrant was overbroad in seeking information about Bickle's associations, or in failing to contain necessary language to prohibit the government's access to

privileged attorney-client communications or attorney work-product. However, even if the warrant is overbroad, the remedy is to suppress only the items seized pursuant to the overbroad portions of the warrant. The government maintains that Bickle fails to recognize the complexity of segregating electronic data and ignores applicable Ninth Circuit case law regarding association information and provisions in the search warrant that limit information that can be seized.

In this case, the warrant only sought information pertaining to Bickle's association which constitute fruits, evidence and instrumentalities of violations of specific enumerated statutes in which Bickle and members of his conspiracy were involved. As such, the warrant is not overbroad. The government also points out that the affidavit supporting the search warrant requested emails from March 1, 2009, the same month that Bickle allegedly smuggled the majority of firearms at issue in this case into the country. Additionally, because the government had information that Bickle continued to use his email account to contact people regarding a conspiracy after his arrest, the search warrant is not temporally overbroad by seeking information after November 4, 2010.

The government also asserts that the warrant is not overbroad in scope because it failed to contain necessary language identifying emails and files constituting attorney-client communications or attorney work-product. The government contends that Microsoft informed ATF that they could not or would not sort files to withhold information regarding Bickle's legal representation. Additionally, the Ninth Circuit has authorized use of the filter agent process as an appropriate means for the prosecution to insulate itself from potentially confidential materials.

Finally, the government maintains Bickle has not established that there were any false or misleading statements in the affidavit which would entitle him to a *Franks* hearing. The portions of the warrant Bickle cites in support of his request do not establish a single, false statement was made, and the motion makes only a vague allegation that false statements were made knowingly, intentionally or with reckless disregard for the truth. Bickle's request for a *Franks* hearing is not accompanied by an affidavit or other reliable statements supporting his conclusory and baseless statements. For example, the affidavit did not mislead the court into believing that Bickle sold guns to an undercover ATF officer. Rather, the government had substantial evidence that Bickle was part of a conspiracy that "sold or otherwise distributed" firearms to an ATF officer and stated this in the affidavit. Bickle's citation to

the affidavit's reference to the Klier emails is also insufficient to establish that the government made false or misleading statements or omissions knowingly, intentionally, or with reckless disregard for the truth.

Although the government maintains that the warrant contained probable cause for the items authorized to be searched for and seized, if the court disagrees, the evidence is admissible under the good faith exception to the exclusionary rule. In this case, the affidavit reflects the government had overwhelming evidence that linked Bickle to illegal transportation of firearms. Therefore, even if the warrant lacked probable cause or was overbroad, the court should deny the motion to suppress evidence. The government also argues that, even if the warrant lacked probable cause or was overbroad, the court should deny the motion to suppress based on the inevitable discovery exception to the exclusionary rule. The government acknowledges that it must establish by a preponderance of the evidence that it would have ultimately or inevitably discovered the same evidence pursuant to the warrant. The government asserts that, because it seized the Defendant's cellular telephone which had email information stored on it that, "to the extent that email account information stored on Defendant's seized telephone overlaps with e–mail account information obtained through the search at issue here, the court should not suppress that information."

C. Bickle's Reply (Dkt. #110)

Bickle replies that the government's justifications for the warrant lack substance and that there are no facts in the affidavit supporting the conclusion that evidence of crimes would be found in Bickle's Hotmail account. The warrant is overbroad because it authorized seizure of the contents of all emails sent to and from the account, as well as Bickle's entire contact list, calendar data, and personal pictures, data, or files found in the account. This authorized a general exploratory rummaging of his private communications in violation of the Fourth Amendment.

Bickle also reiterates his arguments that the government ignored its own filtering procedures because Microsoft directly delivered the disk to the lead ATF agent involved in this case. Additionally, although the affidavit provided that potentially-privileged materials would be placed in a sealed envelope and shared with defense counsel, "it is unclear how that could possibly work because of the format in which the emails were disclosed by Microsoft," *i.e.* they were provided in electronic format

on a CD. Because privileged and non-privileged materials are mixed together, the only way the filtering process could work would be if the filter agent printed out hard copies of the data and only provided non-privileged emails in hard copy to the government. Because counsel for Bickle has not received any communication from counsel for the government concerning whether potentially privileged emails were removed from the government's copy, the government continues to circumvent the filtering procedures required by the Ninth Circuit as described in *United States v. Danielson*, 325 F.3d, 1054, 1071-72 (9th Cir. 2003).

Finally, Bickle argues he is entitled to a *Franks* hearing because the entire affidavit submitted to Judge Foley "is riddled with omissions and conclusions based on speculation" and was a clear attempt to mislead him into finding probable cause where there was none.

II. The May 13, 2011, Hearing.

The government's opposition to the motion to suppress did not address with any specificity Bickle's arguments that the government did not follow the filter procedures outlined in the warrant. As a result, the court set the matter for oral argument and directed that the government be prepared to address, in detail, the filter procedures that were followed in this case. At the May 13, 2011, hearing, Mr. Pokorny, counsel for Bickle, outlined the chronology of what occurred. Bickle was arrested November 3, 2010, and a month later the government sent a preservation letter to Microsoft requesting that the contents of any communications in the account be preserved. The preservation letter stated that if Microsoft had any questions or data, it should call the then-assigned AUSA Drew Smith, or Eric Fox. On December 6, 2010, Microsoft responded indicating it would preserve data pursuant to the statute for ninety days. The letter was addressed to the U.S. Attorney's Office, Attn: Eric Fox. On January 18, 2011, the warrant was submitted to Judge Foley and issued and served on Microsoft the same day.

Counsel for Bickle indicated it was a mystery to the defense why the warrant was presented to Judge Foley rather than the undersigned. The court advised counsel that the local practice in this district is for any applications for search warrants to be presented to the presiding duty judge and that Judge Foley was on duty the week the warrant was issued.

Counsel for Bickle then addressed the affidavit supporting the search warrant and pointed out that out of the forty-four paragraphs, three of them talk about the filtering of potentially privileged

materials. In essence, the warrant required a filter agent to be assigned from ATF to review the materials and remove anything potentially privileged. Any questions the filter agent had were to be directed to the U.S. Attorney. If privileged materials were found, they were required to be placed in a sealed envelope for immediate return to Bickle or his attorney. Defense counsel could then determine whether to assert a claim of privilege, and if there was a difference of opinion, the matter would be submitted *in camera* to a neutral third party, such as a magistrate judge.

On February 2, 2011, Eric Fox received a CD from Microsoft.[1] The following day it was assigned an evidence identification label and marked as Exhibit 179. The same day, Mr. Pokorny had a meeting set up with the U.S. Attorney's Office in Las Vegas with AUSAs Greg Damm and Phil Smith and ATF Agent Tom Chittam regarding discovery issues. At the meeting, Mr. Pokorny was given a CD marked "Bickle email warrant." The following day, he faxed a letter to Mr. Damm indicating he was unable to access materials on the CD. Five days later, he received an email with a password to access the emails. Two days later, he sent a letter to Mr. Damm expressing serious concern because attorney-client communications were on the CD. Four days after that, Mr. Damm sent Mr. Pokorny a letter assuring him that no Sixth Amendment violations had occurred.

On February 17, 2011, the government filed a motion to unseal the search warrant and affidavit, and on February 22, 2011, Mr. Pokorny received the affidavit and warrant.

Mr. Pokorny and his assistant "spent a considerable amount of time" going through the contents of the CD. They found that there were 1,441 emails from April 11, 2006, through February 1, 2011. The email account was opened shortly before April 11, 2006. Of the 1,441 emails, 231 emails were dated from November 3, 2010, the date of Bickle's arrest, through February 1, 2011, when Microsoft complied with the warrant. Mr. Pokorny believes ninety emails on the CD are privileged. All but five of the ninety emails are between Mr. Bickle and Mr. Pokorny. The other five are between Mr. Bickle and Mr. Pokorny's research attorney, Crystal Walser, and between Mr. Bickle and a doctor he was

---

[1]The lawyers indicated the information from Microsoft was contained on a CD. At the June 10, 2011, evidentiary hearing, Special Agent Fox clarified that he received an email from Microsoft containing a link to the information from Bickle's email account. He then burned the information from the link onto a DVD because the amount of data was too large to put on a CD.

consulting with for mental health purposes. The motion to suppress was filed March 9, 2011, after counsel had an opportunity to review the contents of the CD provided by the government. Mr. Pokorny argued that the government's access to privileged communications was prejudicial and cited examples of how his defense had been prejudiced. One of the emails on the CD is dated January 27, 2011, and contains Mr. Bickle's notes and impressions of various reports contained in discovery. Emails dated January 24 and 25, 2011, contain discussions between Bickle and Mr. Pokorny regarding possible plea negotiations. On January 18, 2011, there are memos between Mr. Bickle, Ms. Walser, and the defense ATF consultant regarding discovery issues which are clearly work product. There are December 30, 2010, and January 11, 2011, emails, with the mental health care professional involved in this matter. There were also email exchanges between Mr. Bickle and his counsel on December 22, 2010, regarding plea negotiations.

Counsel for Bickle argued that the government has run "roughshod" over Mr. Bickle's Sixth Amendment rights and that the government must have understood that Bickle would be communicating with his counsel by email because of the strict conditions imposed on his release which included confinement to base and GPS monitoring.

Counsel for the government made representations to clarify the taint[2] procedure that the government utilized in this case. In summary, Mr. Damm represented that Microsoft was instructed to send the response to the search warrant to the case agent to preserve the chain of custody. The CD received from Microsoft was received by the case agent, marked and placed in the ATF evidence vault in Las Vegas where it remains. Mr. Damm assured the court and opposing counsel that the case agent had not reviewed the contents of the CD. An Intelligence Research Specialist, Debra Martinez, with the San Francisco field office of ATF in Dublin, California, was selected to serve as the taint agent. Instructions to the taint agent were a "collaborative effort" between the assigned AUSAs and the case agent, Eric Fox, who communicated these instructions to her. The AUSAs also consulted with Mr. Pokorny, counsel for Bickle, to identify whether anything on the CD provided by Microsoft contained

[2]The transcript of the hearing contains a typographical or transcription error. Page 9, line 7 transcribes Mr. Damm as referring to a "tape" procedure rather than a "taint" procedure.

privileged information. Mr. Pokorny provided the name of his assistant and the name of the physician that Mr. Bickle was consulting with. These names were provided to the taint agent who prepared spreadsheets that were marked as Government's Exhibit "11" and provided to the court and opposing counsel. The spreadsheets identify emails with the names of Mr. Pokorny, his assistant, or the physician.

Mr. Damm indicated that he understood that no one had reviewed the privileged communications and that the spreadsheets were prepared by the taint agent from header information identifying recipient and sender. Mr. Damm took the position that the government complied with the filter procedure outlined in the warrant approved by Judge Foley by providing defense counsel with the entire CD containing not only privileged communications, but also all other emails in Bickle's Hotmail account. Because all of the emails were on one disk, it was not possible to segregate the privileged from the non-privileged materials. He characterized the search warrant filter protocol as one designed for the "paper world" rather than the "electronic world." Counsel for the government represented that neither the case agent nor the filter agent opened or reviewed the content of any communications containing the three names that Mr. Pokorny provided.

Mr. Damm also explained that the warrant only sought email communications beginning March 2009, through the date of the application. However, Microsoft sent a disk containing emails dating back to April 2006, and Mr. Damm indicated he had no idea how that happened. However, he was also aware that an inquiry was made of Microsoft concerning whether it could perform any sort of segregation or filter process, and the government was told it would not. Mr. Damm indicated the government was prepared to stipulate that it would not seek to use, use, or seek to admit any evidence on the disk prior to March 2009.

After hearing the government's representations, the court initially required the government to submit the affidavits of the case agent and the filter agent describing, with specificity, everything that had been done with the disk once it was provided to Special Agent Fox and the filter agent. However, Mr. Pokorny indicated that Mr. Damm's representations were not contained in the government's response, and he was hearing a lot of factual information for the first time. He requested an evidentiary hearing with an opportunity to examine the filter agent. He also indicated that, in briefly reviewing the

spreadsheets marked as Government's Exhibit "1," they contained eighty-one communications; however, he had identified ninety privileged communications on the disk. The court granted his request indicating a limited evidentiary hearing would be conducted to allow counsel to cross-examine on the taint procedures, and to make sure that the government has not accessed privileged communications. The court directed counsel to determine the availability of the case agent and filter agent and to coordinate a mutually agreeable date and time with the court for the hearing on the earliest possible date.

III. The June 13, 2011, Evidentiary Hearing.

At the hearing conducted June 13, 2011, Special Agent Eric Fox, and the filter agent, Debra Martinez, testified. Special Agent Fox testified that on February 1, or February 2, 2011, he received an email from Microsoft which attached a winzip file for Bickle's email account in response to the search warrant. He opened the file to see if it worked and made DVD copies of the contents of the winzip file for government counsel, Mr. Pokorny, and the filter agent. The original DVD was marked with an exhibit sticker and placed in the ATF evidence vault to preserve chain of custody. He discussed with his supervisor who should be selected to serve as the filter agent, and the decision was made to put someone who was disinterested in the investigation in the Bay area involved. He has not seen the content of any of the emails, and has not looked at any privileged emails.

On cross-examination, Special Agent Fox testified that winzip is a file extension that consists basically of a digital filing cabinet. It is compression software. When the file was sent by Microsoft, a password was needed to "unzip" the file. The password was only good for a very short period of time. He copied or "burned" the contents of the winzip file sent by Microsoft. The original or first DVD was placed in the ATF evidence vault to maintain chain of custody. He indicated he believed Ms. Martinez was a disinterested person because she works in California in the Bay area and was removed from the investigation. She had minimal or no knowledge of the case which is why ATF and government counsel concluded she was an appropriate filter agent. Additionally, she was selected because she is known as a hard worker and reliable. Fox set Martinez a copy of the warrant and filter process. However, she was instructed not to begin until the government received a response from Mr. Pokorny identifying individuals who had privileged communications with Bickle.

This was the first email search warrant Special Agent Fox had ever done. The request for a warrant was originally submitted to Judge Foley without a filter process. Fox received a call from AUSA Drew Smith indicating the judge would not approve the warrant without a filter process. Special Agent Fox does not know who drafted the three paragraphs outlining the filter process. He did not. He had never used a filter agent before. He believes that Ms. Martinez followed the process outlined in the warrant, but acknowledged that privileged communications were not physically segregated from the disk and provided to Mr. Pokorny. Martinez was told she could not delete emails on the disk. Ms. Martinez was instructed that if she saw Mr. Pokorny's name, the name of his assistant, or the doctor, that she should not open the email. If Martinez had a question, she would contact Fox who would in turn contact AUSA Damm or Phil Smith. Fox would then relay their instructions to Martinez. Fox served as the point of contact because he was the case agent.

Fox testified that he expected a ream of paper from Microsoft rather than an electronic file. He has served search warrants on banks and other financial institutions who maintain records electronically, but he has always received paper files in response.

Martinez has not separated anything or given anything to Fox. Martinez did send an Excel spreadsheet to him asking if the format was something he could work with. He testified that he had not seen anything else, and "it's kind of frustrating." Martinez discussed the content of one email with him. It was an October 31, 2008, email from Mr. Bickle's father to Bickle which contained a reference to guns.

The court inquired whether anyone else at ATF had access to the winzip file. Fox testified that when he tried to open the link from Microsoft, he had a problem with his computer. The link was not working, and he needed technical advice because it seemed his network station was having a problem. As a result, he forwarded the email to Special Agent Tyler Olsen to assist him in resolving the technical problem. No one else had access to the winzip file.

Debra Martinez testified that she has been employed by ATF as an Intelligence Research Specialist for eight years. She is not an agent, and her duties are to assist agents by analyzing data and providing other forms of assistance. In this case, she was contacted by Eric Fox and requested to review Bickle's emails. She was instructed not to look at any privileged documents. She believed she

was first contacted March 3, 2011, and was sent a copy of the search warrant. Special Agent Fox asked her to review the procedures for the taint process. Agent Fox told her that Mr. Pokorny was Bickle's attorney and that she should not look at anything with his name on it. Fox also told her he would get back to her with other names. She loaded the disk on the hard drive of her laptop because working on the disk itself was hard and time-consuming. She did not begin looking at the content of anything on the disk for one or two weeks until after receiving names of those who had privileged communications with Bickle. She understood the government was waiting for Mr. Pokorny to provide those names. She implemented a procedure to segregate privileged from non-privileged emails on the disk. She testified it was a difficult process. She placed emails with the names Pokorny, Walser or Dr. Johnson on a spreadsheet. She did not view the contents of any emails with their names. Rather, she collected these emails and placed them on her spreadsheet by looking at the header information. She prepared a PowerPoint presentation to demonstrate the step-by-step process she followed. Copies of the eleven slides used in her PowerPoint presentation were marked and admitted as government's Exhibit "2" at the hearing.

On cross examination, she testified that she had a questions concerning whether she should look at and print out the privileged emails like the search warrant says. She received a response from AUSA Damm who told her not to do so, to ensure that she did not go into any privileged documents.

When asked whether she had any prior involvement with Bickle's case, she testified "no, not really." She did recognize his name because, during the time of his arrest, an ATF command post was set up. She was not present during any of the arrests, but was in the Dublin command post available to assist ATF agents in the field. The procedure is for agents to call the command post when they have made an arrest. Agents may also request people at the command post to do computer research to assist the investigation. She has a Bachelor of Arts in Criminal Justice and is generally familiar with the attorney-client privilege. She testified that it consists of communications between the client and an attorney for the benefit of the Defendant, and is important to ensure a fair trial. She was designated as a taint or filter agent on one prior occasion in 2010. The other case involved both electronic and paper files. She is not sure what, if any, procedures ATF has to select a taint or filter agent.

/ / /

She was not told about the temporal limitation of the search warrant until the date of the last hearing in this case, May 13, 2011. Although she received a copy of the application for the search warrant, she only reviewed those portions pertaining to the filter procedures. She sent an email to Special Agent Fox about an email between Bickle and his father dated October 31, 2008, because she thought it was significant because it discussed a "Russian 47."

On redirect, she reiterated that she filtered all attorney-client and doctor-client communications by placing them on her spreadsheet from header information contained on the disk she received. She found one email from Bickle to his sister that had the same subject line as the subject line of one of the emails between Mr. Bickle and Mr. Pokorny. She asked for clarification and was told to treat it as privileged. She did not go into the email between Bickle and his sister and does not know its content. It has taken her more than three months to get halfway through the filter process. However, now that she has been told to limit her review to emails beginning in March 2009, the time frame for completing her work should drop dramatically.

III. Law and Analysis.

The Fourth Amendment secures "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures." U.S. Const. amend. IV. The Fourth Amendment protects reasonable and legitimate expectations of privacy. *Katz v. United States*, 389 U.S. 347 (1967). The Fourth Amendment protects "people not places." *Id*. Evidence obtained in violation of the Fourth Amendment, and evidence derived from it may be suppressed as the "fruit of the poisonous tree." *Wong Sun v. United States*, 371 U.S. 471 (1963).

A person must have a reasonable expectation of privacy in the place searched to claim a violation of his or her Fourth Amendment rights. The Supreme Court has enunciated a two-part test to determine whether an expectation of privacy is reasonable and legitimate. *See Katz*, 389 U.S. at 361. First, the individual must have an actual subjective expectation of privacy, and second, society must recognize that expectation as objectively reasonable. *Id*. The government does not challenge Bickle's assertion that he had a reasonable and legitimate expectation to privacy in the contents of his email account.

/ / /

A. Defendant's Request for *Franks* Hearing.

In *Franks v. Delaware*, 438 U.S. 154 (1978), the Supreme Court addressed at length whether a false statement by a government affiant invalidates a search warrant. *United States v. Hammett*, 236 F.3d 1054, 1058 (9th Cir. 2001). In *Franks*, the Court held that a defendant could challenge a facially valid affidavit by making a substantial preliminary showing that "(1) the affidavit contains intentionally or recklessly false statements, and (2) the affidavit purged of its falsities would not be sufficient to support a finding of probable cause." *United States v. Lefkowitz*, 618 F.2d 1313, 1317 (9th Cir.), *cert. denied*, 449 U.S. 824 (1980). *See also United States v. Stanert*, 762 F.2d 775, 780 (9th Cir. 1985). Pursuant to *Franks*, "[t]here must be allegations of deliberate falsehood or reckless disregard for the truth, and these allegations must be accompanied by an offer of proof." *Hammett*, 236 F.3d at 1058 (*quoting Franks*, 438 U.S. at 171). Where the defendant makes such a showing, the Fourth Amendment requires that a hearing be held at a defendant's request. *Franks*, 438 U.S. at 155-56; *Stanert*, 762 F.2d at 780**.**

Bickle contends the affidavit in support of the search warrant is intentionally misleading and contains statements without which probable cause would not exist to issue the search warrant. Bickle asserts that the affidavit wrongfully portrays Bickle as having sold guns to an undercover ATF agent when it states, "at least three co-conspirators . . . and Bickle sold or otherwise distributed factory made machine guns that have origins in Iraq, to an undercover ATF Task Force Officer." Bickle asserts the government has no information to believe Bickle ever sold guns to an ATF agent. The affidavit also misleads the court into inferring that Bickle tampered with witnesses through his email account when it states the affiant "knows of other instances in which Bickle utilized polarbickle@hotmail.com to email people who could potentially be witnesses. . . . Such emails could potentially be evidence of attempts to obstruct justice." The affidavit then refers to an email in which Bickle tells witness Matt Klier "some guys have opted [for] lawyers and have ben [sic] left alone." Further, Bickle contends information concerning payments to Mr. Klier were misrepresented as possible payments for guns, when the government was aware, based upon Mr. Klier's affidavit, that payments made by Bickle were for repair work to Bickle's motorcycle. He also asserts that paragraph 27 of the warrant wrongfully suggests Bickle used his email and text messages to sell guns to Jason Cole.

The court finds Bickle has not met his burden of establishing that the affidavit contains deliberate falsehoods or statements made with reckless disregard for the truth. Although Bickle has specifically challenged certain portions of the warrant, he has not established the statements he challenges were false or misleading. A fair reading of the affidavit does not suggest the government claimed Bickle sold guns directly to an undercover ATF officer. Rather, the affidavit clearly articulates the government's theory of the case that Bickle was involved in a conspiracy with at least three co-conspirators to sell or distribute factory-made guns that had origins in Iraq to an undercover ATF Task Force Officer and other civilians. Nor is the affidavit misleading about the government's belief that Bickle was communicating with potential witnesses to persuade them not to cooperate with the government. The affidavit relates the content of certain messages and relates them to other events supporting the government's conclusion that they were sent in an effort to persuade potential witnesses not to cooperate. Reasonable minds may differ concerning whether the emails referred to in the affidavit were innocent or inculpatory. However, this does not make statements concerning these communications false or misleading.

Finally, the affidavit is not misleading concerning the $800 payment to Klier. The affidavit relates that Klier told an ATF agent that the $800 wire transfer was for a motorcycle part transaction. Fox explained this was significant to him because on October 10, 2010, one day after an undercover ATF officer paid $8,000 to purchase guns from co-conspirator Richard Paul, Paul and Bickle communicated by emails. Bickle instructed Paul that, if asked about the $8,000.00 wire transfer by officials, he should explain it as payment for a motorcycle. Accordingly, Bickle's request for a *Franks* hearing is denied.

B. Scope of Warrant: Overbreadth and Particularity.

The warrant clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one particularly describing the place to be searched and the persons or things to be seized. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). The purpose of the particularity requirement is to prevent general searches. *Id*. By limiting the authorization to search the specific areas and things for which there is probable cause to search, the particularity requirement ensures that the search will be

/ / /

carefully tailored to its justifications, and will not become a wide-ranging, exploratory search the Fourth Amendment prohibits. *Id.*

"[T]he scope of a lawful search is 'defined by the object of the search.'" *United States v. Ewain*, 88 F.3d 689, 692 (9th Cir. 1996) (*quoting Maryland v. Garrison*, 480 U.S. 79, 84 (1987)). The test is an objective one: "would a reasonable officer have interpreted the warrant to permit the search at issue." *United States v. Gorman*, 104 F.3d 272, 274 (9th Cir. 1996). *See also United States v. Leon*, 468 U.S. 897, 918-19 (1984); *United States v. Traylor*, 656 F.2d 1326, 1331 (9th Cir. 1981). Search warrants must be specific. *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006). "Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *Id.* (*citing United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993)).

The warrant's description of items need only be "reasonably specific, rather than elaborately detailed." *Id. (citing United States v. Storage Spaces Designated Nos. 8 & 49,* 777 F.2d 1363, 1368 (9th Cir. 1985), *cert. denied,* 479 U.S. 1086 (1987) (internal citation omitted)); *see also United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986) (the level of detail necessary in a warrant is related to the particular circumstances and the nature of the evidence sought). "Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible." *Id.* The level of specificity required "varies depending on the circumstances of the case and the type of items involved." *Id.*

In determining whether a warrant is sufficiently particular, the Ninth Circuit considers one or more of the following factors: (1) whether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant sets out objective standards by which the executing officers can differentiate items subject to seizure from those which are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued. *Id.*

Here, the warrant directed Microsoft to **disclose** to the government the following information:

(a) The contents of all emails stored in the account, including copies of emails sent to and

from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

(b) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

(c) All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

(d) All records pertaining to communications between Microsoft Corporation and any person regarding the account, including contacts with support services and records of action taken.

Exhibit A to Motion to Suppress at 18:4-21.

Although AUSA Damm argued at the May 13, 2011, hearing he had "no idea" why Microsoft provided electronically stored information dating back to 2006 when the account was opened, a plain reading of the warrant indicates this is what the government applied for and what Judge Foley authorized to be disclosed. There was no temporal limitation imposed in the warrant regarding what Microsoft was obligated to disclose. Rather, the temporal limitation of March 1, 2009, to the present (date of execution of the warrant) was imposed for that which the government was authorized to **seize.**

Particularity is not the problem with the warrant in this case. The warrant called for Microsoft to disclose all records and information in Microsoft's possession associated with polarbickle@hotmail.com. It is not ambiguous concerning what was sought. Rather, the question is whether the warrant is overbroad in authorizing Microsoft to disclose all account information and content while temporally and subject matter limiting what the government what the government was

///

authorized to seize.[3] The purpose of the Fourth Amendment's particularity requirement is to make general searches impossible and prevent "exploratory rummaging in a person's belongings." *See United States v. Rodriguez*, 869 F.2d 479, 486 (9th Cir. 1989) (*citing Andresen v. Maryland,* 427 U.S. 463, 480 (1976)). The need to prevent general exploratory rummaging of a person's belongings is particularly acute in document searches because, unlike requests for other tangibles, document searches tend to involve broad disclosures of the intimacies of private lives, thoughts, and transactions. *United States v. Washington*, 797 F.2d 1461, 1468 (9th Cir. 1986) (internal citations and quotations omitted). However, the Ninth Circuit has often recognized a legitimate law enforcement need to scoop up large quantities of data and sift through it carefully for concealed or disguised pieces of evidence. *See*, *e.g.*, *United States v. Hill*, 459 F.3d 966 (9th Cir. 2006).

Mr. Pokorny has had his copy of the DVD containing the content of what Microsoft forwarded since February 1 or 2, 2011, and he does not claim that the DVD he received contains anything other than emails. The court has no information concerning whether Microsoft disclosed all of the account information required by the warrant. This report of findings and recommendation will therefore not address issues not raised in the papers, in oral argument, or at the evidentiary hearing.

C. 18 U.S.C. § 2703.

As a preliminary matter, the affidavit supporting the application for a search warrant in this case sought authorization for the contents of Bickle's email account pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A). 18 U.S.C. § 2703(a) governs obtaining the contents of wire or electronic communications in electronic storage. It permits a government entity to require a provider of electronic services to disclose the contents of a wire or electronic communication that is in electronic storage in an electronic communication system for 180 days or less pursuant to a warrant issued in compliance with the Federal Rules of Civil Procedure. 18 U.S.C. § 2703(a). It also authorizes a government entity to require a provider of electronic communication services to disclose the contents of wire or electronic communications that have been in electronic storage in an electronic communication

[3]Neither counsel for Bickle, nor the government, provided the court with a copy of the search warrant return or addressed whether Microsoft provided anything than the 1,441 emails sent electronically to Special Agent Fox which he "burned" on DVDs.

system for more than 180 days following the procedures outlined in subsection (b). *Id*. Section 2703(b)(1)(A) authorizes a government entity to require a provider of remote computing services to disclose the contents of any wire or electronic communication without notice to the subscriber or customer if the government obtains a warrant issued pursuant to the Federal Rules of Criminal Procedure. Section 2703(c)(1)(A) authorizes a government entity to require a provider of electronic communication service or remote computing service to disclose records or other information pertaining to a subscriber or customer if the government obtains a warrant issued pursuant to the Federal Rules of Criminal Procedure.

18 U.S.C. § 2703(f)(1) requires a provider of wire or electronic communication services or a remote computing service to take necessary steps to preserve records and other evidence in its possession pending issuance of a court order or other process upon the request of a government entity. The provider is required to retain the records referred to in 2703(f)(1) for a period of ninety days. In this case, it is undisputed that the government sent a preservation letter to Microsoft in December 2010, requesting that the contents of any communications in Bickle's Hotmail account be preserved. Microsoft responded in a letter dated December 6, 2010, that it would preserve data pursuant to the statute for ninety days. After the government sent the preservation letter, and Microsoft agreed to comply, Special Agent Fox applied for the warrant at issue in this case. The warrant was served on Microsoft, which gathered the information and forwarded it to Special Agent Fox in an email a password-protected internet link. A law enforcement officer is not required to be present during the service or execution of a search warrant issued in accordance with § 2703. 18 U.S.C. § 2703(g).

During oral argument at the May 13, 2011 hearing, counsel for Bickle acknowledged that the presence of a law enforcement officer was not required for service or execution of the search warrant and conceded that the government had met the statutory "minimum requirements." However, counsel for Bickle argued that the government should not have directed that Microsoft comply with the warrant by sending the content information to the case agent and/or the prosecutors involved in this case. Rather, he maintained the information could have, and should have, been forwarded directly to the filter agent. Government counsel explained that the case agent was designated to receive the response to the warrant because of the necessity for maintaining chain of custody.

Counsel for Bickle was not aware, until the government made its representations at the May 13, 2011 hearing, what procedures were followed to ensure that government counsel and the case agents or investigating officers did not have access to the information Microsoft provided before it was filtered and segregated to exclude privileged communications. Because the government did not dispute that there were privileged communications in the emails Microsoft provided, the court granted counsel for Bickle's request for an evidentiary hearing to cross-examine the case agent and filter agent to fully develop the record about what actually occurred.

After hearing their testimony on direct, and being afforded an opportunity to cross examine Special Agent Fox and Ms. Martinez, Mr. Pokorny stated he had no reason to doubt their integrity. However, he emphasized that the government did not follow the taint procedure mandated in the warrant, and DVD copies of the contents of Bickle's account which contain privileged materials have been in the possession of the prosecutors and the case agent since Microsoft complied with the warrant. Because of the number of privileged communications on the DVDs counsel for Bickle argued the filter procedures the government implemented were inadequate, and that the court should suppress everything contained on the DVDs.

The court finds that both Special Agent Fox and Ms. Martinez were credible in their testimony. Specifically, the court believes Special Agent Fox's testimony that he has not opened or read the contents of any of the emails contained in the link he received from Microsoft. The court accepts his testimony that he copied the contents of the materials received from Microsoft on DVDs making one copy, which was marked with an Exhibit sticker and placed in the ATF vault to preserve the chain of custody, and also made a copy for the prosecutors, a copy for Mr. Pokorny, and a copy for the filter agent. The court finds Ms. Martinez credible concerning the procedures she implemented to segregate privileged emails from non-privileged emails on the disk. Specifically, the court found her credible that she placed all emails with the names Pokorny, Walser, or Dr. Johnson on a spreadsheet and did not review the contents of any emails with their names. Rather, she collected these emails and identified them on her spreadsheet by looking at header information identifying who sent or received them.

The filter procedures directed by Judge Foley were intended to restrict how the seized contents of Bickle's email account were to be handled. The purpose of these procedures was to ensure that

privileged communications between Bickle and his counsel would not fall into the hands of government prosecutors or investigating agents. As indicated, the court has found that neither Special Agent Fox nor Ms. Martinez have reviewed the contents of any privileged communications. However, it is undisputed that Ms. Martinez did not comply with the filter procedure outlined in paragraph 41 of the application for the warrant. That paragraph provided that if any privileged materials were found they would be placed in a sealed envelope for immediate return to Bickle or his attorney. AUSA Damm explained that this procedure was not literally followed because the filter procedure was designed for a paper response rather than an electronic response to the warrant. Special Agent Fox testified that this was his first email search warrant and that he expected a paper response from Microsoft. The court found him credible in this regard.

Ms. Martinez read paragraph 41 and was aware that it required her to place any privileged communications in a sealed envelope for return to Bickle and/or his counsel. She sought direction from AUSA Damm through Special Agent Fox and was directed not to print out the electronic files because she would have to open them to do so.

During the May 13, 2011, hearing, AUSA Damm reasoned that having Martinez open the electronic records to print a hard copy would create a bigger risk of government access to the contents of the privileged communications than recording the privileged communications on a spreadsheet without opening or accessing the content. He also concluded that because Mr. Pokorny had identified all individuals who would have been involved in privileged communications with Bickle, and because Pokorny had a DVD copy of everything Microsoft sent, that this provided superior segregation or filtering than the procedure outlined in the warrant.

Faced with this dilemma, the government should have applied to the court for an amendment to the filtering procedures the warrant mandated. The government was not at liberty to substitute another procedure for the one the court directed. However, the court agrees that having a government agent open privileged communications to print them out and return them in a sealed envelope to defense counsel would give the filter agent more access to the privileged communications than she has had. Additionally, the court agrees that because the purpose of the filter procedures was to prevent government access to privileged communications, and because defense counsel had the DVD

containing everything Microsoft provided, and was asked to identify all individuals having privileged communications with Bickle, that it made little sense to print and return paper copies of electronic records defense counsel already had. Nevertheless, the government applied for judicial authorization to obtain the contents of the email account, received judicial direction concerning how privileged materials should be handled, and should have sought judicial authorization for an amendment to the procedures Judge Foley directed when compliance became problematic. Having received judicial authorization and direction, the government was not at liberty to ignore the court's direction or substitute its own plan for what Judge Foley mandated. However, for reasons discussed below, the court finds that suppression of everything the warrant authorized the government to seize is not the appropriate remedy for the government's failure to comply with the filter procedure outlined in paragraph 41 of the application for the warrant.

During the May 13, 2011, hearing, government counsel conceded that any emails predating March 1, 2009, were outside the scope of what the warrant authorized the government to seize, and partial suppression of emails predating March 1, 2009, was the appropriate remedy. The court agrees that partial suppression of the contents of Bickle's email account dated earlier than March 1, 2009, should be ordered. The court will also recommend that the government should not be permitted use, for any purpose, emails dated prior to March 1, 2009.

The warrant authorized the government to **seize** all information disclosed by Microsoft that constitutes fruits, evidence, and instrumentalities of violation of 18 U.S.C. §§ 2, 371, 842(a)(3)(A), 922(o) and 26 U.S.C. §§ 5861(d), 5861(e), 5861(j), 5861(k) (together, the "Subject Offenses") involving Bickle or other known or unknown members of the conspiracy since March 1, 2009, including for each account or identifier, information pertaining to the following matters:

(a) Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

(b) Communications and records that may establish ownership and control (or the degree thereof) of the email accounts to be searched, including address books, contact or buddy lists, bills, invoices, receipts, registration records, bills, correspondence, notes, records, memoranda, telephone/address books, photographs, video recordings, audio recordings,

lists of names, records of payment for access to newsgroups or other online subscription services, and attachments to emails, including documents, pictures, and files,

(c) Communications and records regarding communications between the email account user and the provider's support services including complaints from or about other users, technical problems or billing inquiries;

(d) Communications and records that may be related to the Subject Offenses;

(e) Communications and records regarding financial transactions that may reflect the transfer of proceeds of the Subject Offenses;

(f) Communications and records that may show persons, corporations or other artificial entities that may be holding proceeds of the Subject Offenses;

(g) Communications and records that may show co-conspirators of the Subject Offenses and their roles;

(h) Records regarding chat forum discussions that may pertain to the Subject Offenses;

(I) Communications and records that evidence other email accounts that may relate to the Subject Offenses;

(j) Communications and records that may show motivation for engaging in the Subject Offenses; and

(k) Communications and records regarding the Subject Offenses.

Neither the government nor Bickle has cited any case deciding a Fourth Amendment challenge to a warrant for electronically stored information served on an internet service provider on particularity or breadth grounds. The court's research found only two published decsions–both of which upheld searches for all emails in a user's account. *See, e.g., United States v. Bowen,* 689 F.Supp.2d 675, 682 (S.D.N.Y. 2010) (stating the Fourth Amendment does not require the executing officers to delegate a pre-screening function to the internet service provider to ascertain which emails are relevant before copies are obtained from the internet service provider for subsequent searching) (*citing United States v. Vilar,* 2007 WL 1075041 at *35 (S.D.N.Y. Apr. 4, 2007) (recognizing that "it is frequently the case with computers that the normal sequence of search and then selective seizure is turned on its head") (internal citation and quotation marks omitted)); *United States v. McDarrah,* 2006 WL 1997638

(S.D.N.Y. 2006) (upholding warrant for search of all email and stored content against an overbreadth/particularity challenge).

However, there is a well-developed body of Fourth Amendment law addressing the search and seizure of large quantities of materials to review and sort the material for items within the scope of probable cause underlying the warrant. For example, in *Andreson v. Maryland*, 427 U.S. 463, 482 n.11 (1976), the Supreme Court recognized that, "[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." Because computers typically contain so much information outside the scope of the criminal investigation, computer searches raise difficult Fourth Amendment issues not encountered in searches of paper files. *United States v. Adjani*, 452F.3d 1140 (9th Cir. 2006) (holding district court properly admitted evidence of child pornography on defendant's computer storage media notwithstanding the lack of a sufficiently detailed supporting affidavit describing the need for wholesale seizure of such media).

The Ninth Circuit has recently and exhaustively addressed search warrants for computer and electronically stored information in a series of decisions involving grand jury investigations into illegal steroid use by major league baseball players. Three published decisions culminated in an *en banc* decision in *United States v. Comprehensive Drug Testing, Inc.,* 621 F.3d 1162 (9th Cir. 2010) ("CDT III"). There, the Ninth Circuit recognized that data that individuals used to keep in file cabinets in physical facilities are now usually stored electronically, and law enforcement faces many challenges in retrieving electronically stored information. *Id*. at 1175. "Electronic storage facilities intermingle data, making them difficult to retrieve without a thorough understanding of the filing and classification systems used–something that can often only be determined by closely analyzing the data in a controlled environment." Because of these challenges, the Ninth Circuit recognized law enforcement's legitimate need to seize large quantities of data is an inherent part of the electronic search process. *Id*. at 1177. However, the legitimate need of law enforcement for authorization to examine large quantities of electronic records "creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Id*. at 1176.

/ / /

To address these competing concerns, CDT III updated its earlier decision in *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982) "to apply to the daunting realities of electronic searches." *Id*. at 1177. *Tamura* preceded the dawn of the information age and involved the seizure of several boxes and dozens of file drawers of paper documents to be sorted out for documents the search warrant authorized later. CDT III made it clear that the procedural safeguards outlined in the *Tamura* opinion have "provided a workable framework for almost three decades" and should be applied to the realities of electronic searches. Specifically, the Court of Appeals reiterated that wholesale seizure of voluminous documents to be sorted out for documents a search warrant authorizes the government to seize may sometimes be necessary. Although often necessary, the Ninth Circuit continues to disapprove of the wholesale seizure of documents, particularly where the government fails to return materials that were not the object of the search once they have been segregated. *Id*. However, there is no reason to suppress properly-seized materials just because the government took more than authorized by the warrant. *Id*. If records are so intermingled that they cannot feasibly be sorted on site, the government should seal and hold the documents pending approval by a magistrate judge of a further search following the procedures set forth in the American Law Institute's *Model Code of Pre-Arraignment Procedure*. *Id*. If the need for transporting large quantities of information is anticipated, the government should apply for specific authorization for large-scale removal of material, which should be granted by the magistrate judge issuing the warrant only where on-site sorting is not feasible, and no other practical alternatives exist.

In the case of electronically stored information, CDT III called upon judges issuing search warrants to apply *Tamura* procedures to electronically stored information "to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases." *Id*. at 1170. Because of the unique problems inherent in the electronic search process, judicial officers should exercise greater vigilance "in striking the right balance between the government's interests in law enforcement and the right of individuals to be free from unreasonable search and seizures." *Id*. at 1177. The court concluded "the process of segregating electronic data that is seizable from that which is not

/ / /

must not become a vehicle for the government to gain access to data which it has no probable cause to collect."

Here, the warrant authorized Microsoft to disclose *all* emails in Bickle's account and account information, including address books, contact and buddy lists, calendar data, pictures, and files, or evidence of the enumerated crimes without regard to whether they were written during the time frame Bickle is alleged to have engaged in the conspiracy. At the evidentiary hearing, AUSA Damm represented that Microsoft would not perform any sort of segregation or filter process. Although AUSA Damm stated that he was unsure why Microsoft sent the contents of Bickle's email account, it is clear that Microsoft was merely complying with the language of the warrant which directed disclosure of the contents of all emails stored in the account as well as all account information. The court agrees with the decision in *Bowen* that the Fourth Amendment does not require delegation of a pre-screening function to an internet service provider to determine which emails are authorized to be seized before the information is obtained by law enforcement for search and seizure of content the warrant authorized. Although the warrant authorized the government to search the entire contents of Bickle's email account, the government was only permitted to seize items related to the offenses enumerated in the warrant. Moreover, a filter process was mandated by Judge Foley to sort or filter privileged emails from non-privileged emails.

The testimony at the June 10, 2011, hearing clearly established that the filter agent did not read the entire warrant. She only familiarized herself with the three paragraphs about the filter process, and as a result, she was unaware that the warrant contained any temporal or subject matter limitations until the May 13, 2011 hearing. However, the filtering protocol only dealt with filtering attorney-client and work product privileged emails and did not direct the filter agent to screen and segregate email by subject matter. The Ninth Circuit has explicitly permitted the use of a filter agent, unassociated with the prosecution, to screen potentially confidential material. *See United States v. Danielson,* 325 F.3d 1054, 1071-72 (9th Cir. 2003). The purpose of the filter procedure the warrant directed has been accomplished. The filter agent has not opened or read the content of any emails with the names of individuals who had potentially privileged communications with Bickle–nor have government prosecutors or case agents. Counsel for Bickle was asked to identify persons having privileged

communications with Bickle and did so before the filter agent began her review. Government prosecutors and the case agents have not accessed the content of anything on the DVDs copied from the material Microsoft provided. The warrant did not require the filter agent to segregate non privileged emails or account information by date or subject matter.

Although the warrant authorized the government's filter agent to search all non-privileged emails, it only authorized the government to seize certain communications and records from March 1, 2009, forward related to the enumerated offenses and communications and records relating to who created, used, or controlled the email account. Bickle is alleged to have smuggled guns into the country during this time, and the court finds that what the warrant authorized the government to seize is not overbroad as to time. Similarly, the content of emails the government was authorized to seize is also limited by subject matter.

The government concedes it may not use anything Microsoft provided dated prior to March 1, 2009, and that it may not access any of the privileged communications Bickle had with his attorney, his attorney's assistant, or the doctor he consulted for defense purposes. The government does not challenge the privileged nature of any of these communications which have been identified by the filter agent from header information and placed on a spreadsheet.

The court does not find the warrant overly broad in its authorization to obtain account information. The Ninth Circuit has repeatedly upheld warrants authorizing the seizure of items which establish the identity of persons in control of premises. "It is axiomatic that if a warrant sufficiently describes the premises to be searched, this will justify a search of the personal effects therein belonging to the person occupying the premises if those effects might contain the items described in the warrant." *United States v. Gomez-Soto*, 723 F.2d 649, 654 (9th Cir. 1994). The Ninth Circuit has long upheld warrants "authorizing the seizure of items which establish the identity of persons in control of the premises." *United States v. Whitten*, 706 F.2d 1000 (9th Cir. 1983); (*citing United States v. Marques*, 600 F.2d 742, 751 at n. 5 (9th Cir. 1979), *cert. denied*, 444 U.S. 1019 (1980)).

Similarly, seizing information regarding identification of the account, including name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to

register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number) all tends to establish whether the Hotmail account is indeed Bickle's, and whether he was using or accessing the account to commit the enumerated offenses.

The warrant also authorized Microsoft to disclose: (a) information about the account holder of polarbickle@hotmail.com; and (b) all records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files. It essentially seeks all information in the account concerning Bickle's associations, not just those related to co-conspirators or others involved in the enumerated offenses. The Ninth Circuit has held that "[a] warrant to seize evidence of association between a suspect and any other person is patently overbroad." *United States v. Washington,* 797 F.2d 1461, 1473 (9th Cir. 1986). However, because of the way this category of information is electronically stored, there is no way to limit disclosure of this information to people with whom Bickle corresponded since March 2009. The warrant limited the government to seize Bickle's for individuals with whom he has communicated since March 1, 2009, that are related to the enumerated offenses. As such, the warrant is not overly broad in authorizing the seizure of this category of information. *See, e.g., United States v. Rodriguez,* 869 F.2d 479, 487 (9th Cir. 1989) (permitting seizure of evidence of association where the evidence was related to the alleged criminal activity).

C. Good Faith Exception.

When considering the validity of a search warrant, the court may inquire whether the good faith exception applies before determining whether probable cause existed to issue the warrant, or vice versa. *See, e.g., United States v. Huggins,* 299 F.3d 1039, 1047 (9th Cir. 2002) (*citing United States v. Cancelmo*, 64 F.3d 804, 807 (2d Cir. 1995) (stating "[a]pplication of the good faith exception is particularly appropriate [where] the legal question of whether probable cause existed is a close one, while the objective reasonableness of the officers' reliance on the warrant is more straightforward) (internal citation omitted). In *United States v. Leon,* the Supreme Court carved out an exception to the exclusionary rule for a search conducted in good faith reliance upon an objectively reasonable search

warrant. *United States v. Leon,* 468 U.S. 897 (1984). The good faith exception does not apply if: the issuing judge was mislead by information in the affidavit that was knowingly or recklessly false; the issuing judge abandoned his or her detached and neutral judicial role; the affidavit was so lacking in probable cause that no reasonable law enforcement officer could believe it was valid; the warrant was so facially deficient in failing to particularize the place to be searched or the things to be seized that executing officers could not reasonably presume it to be valid. *Id.* The Supreme Court has also held that the good faith exception does not apply when police recklessly maintain or knowingly enter false information into a warrant database to enable future arrests. *Herring v United States*, 129 S. Ct 695. 703 (2009).

Bickle does not claim that the issuing judge abandoned his detached and neutral judicial role, or that the warrant was so lacking in probable cause to render official belief in its existence unreasonable, or that police recklessly maintained or entered false information into a database. The court has found that the warrant met the particularity requirement and was not overbroad in what it authorized the government to seize, and that Bickle has not met his burden of establishing the affidavit contains any knowingly or recklessly false or misleading statements. Thus, even if the affidavit failed to establish probable cause for everything the government received judicial authorization to seize, suppression is not required.

The exclusionary rule is a judicially-created remedy for Fourth Amendment violations, and where police conduct is pursued in good faith, the rule's deterrent function loses much of its force. *United States v. SDI Future Health, Inc.,* 568 F.3d 684, 706 (9th Cir. 2009) (*citing United States v. Luong,* 470 F.3d 898, 902 (9th Cir. 2006). The exclusionary rule's sole purpose is to deter future Fourth Amendment violations. *Davis v. U.S.,* – U.S. – , 2011 WL 236958 at *5 (June 16, 2011). Suppression is not an automatic consequence of a Fourth Amendment violation. *Herring v. United States*, 129 S.Ct. 695, 698 (2009); *see also Illinois v. Gates,* 462 U.S. at 223. Indeed, a long line of Supreme Court cases establish that exclusion has always been the Court's last resort, not its first impulse. *Herring*, 129 S.Ct. at 700 (*citing Hudson v. Michigan*, 547 U.S. 586, 591 (2006)).

Instead, the determination whether suppression is warranted "turns on the culpability of the police and the potential of exclusion to deter wrongful police conduct." *Id.* The extent to which the

exclusionary rule is justified by deterrence principles varies with the culpability of the law enforcement conduct. *Herring,* 129 S.Ct. 701. "Evidence should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." *Id.* (*citing Illinois v. Krull,* 480 U.S. 340, 348-49 (1987)) (internal citation omitted). Generally, "the abuses that gave rise to the exclusionary rule featured intentional conduct that was patently unconstitutional." *Herring,* 129 S.Ct. at 702. To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid to the justice system. *Id.* The exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct. *Id.* Accordingly, when police mistakes are the result of negligence rather than systematic error or reckless disregard of constitutional requirements, any marginal deterrence does not "pay its way." *Id.* In the now famous words of Justice Cardozo, the criminal should not "go free because the constable has blundered." *Id.* at 704 (*citing Leon,* 468 U.S. at 907-08; *People v. Defore,* 242 N.Y. 13, 21 (1926), respectively); *see also Davis,* 2011 WL 2369583 at *6 (when the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs). Isolated, nonrecurring police negligence lacks the culpability required to justify the harsh sanction of exclusion. *Id.* at *7.

Additionally, the benefits of deterrence must outweigh the costs. *See Leon*, 468 U.S. at 910; *Pennsylvania Bd. of Probation and Parole v. Scott,* 524 U.S. 357, 368 (1998) (stating "to the extent that application of the exclusionary rule could possibly provide some incremental deterrent, that possible benefit must be weighed against [its] substantial social costs"). In *Scott*, the Supreme Court commented that the exclusionary rule's "costly toll upon truth-seeking and law enforcement objectives presents a high obstacle for those urging its application." *Id.* at 364-65.

Bickle's reply brief does not address the government's good faith arguments. Rather, he argues that the affidavit supporting the warrant did not state probable cause for everything the government was authorized to seize and therefore overbroad and that the affidavit contains false or misleading statements. He also argues suppression of everything the government received is required because the government did not follow the filter procedures the issuing judge directed.

The warrant contained no temporal or subject matter limitation on what it authorized Microsoft to disclose. However, it did limit what the government was authorized to seize by date and subject matter. The Ninth Circuit has recognized the difficulties that searches of computers and electronically-stored information present. The Ninth Circuit has also acknowledged that law enforcement's legitimate need to seize large quantities of data is an inherent part of the electronic search process. Finally, the Ninth Circuit continues to hold that there is no reason to suppress properly-seized materials because the government took more than was authorized by the warrant. As the Ninth Circuit reiterated in *CDT III*, judges issuing search warrants should apply the *Tamura* framework to the "daunting realities of electronic searches." 621 F.3d at 1177. Wholesale seizures of voluminous documents to be sorted for documents a search warrant authorizes the government to search may sometimes be necessary. However, the government's failure to return materials that were not the object of the search warrant once they have been segregated is disapproved.

The court found Special Agent Fox credible that he had not previously applied for a search warrant for email account information and that he expected to receive paper copies of Bickle's emails. He received an email with a link to an electronic file instead. As AUSA Damm correctly pointed out, the three paragraphs of the warrant containing the filer procedures were designed for the "paper world" rather than the "electronic world." When Microsoft submitted its response to the search warrant in electronic format, the government recognized it could not literally comply with the filter procedures the warrant detailed. The government could have and should have applied to the court for judicial authorization for a modified filter procedure appropriate to the electronic format in which it received the information. However, the government's failure to obtain judicial authorization to modify the approved filter procedure is, at most, negligent. In light of the measures taken to ensure that no one read the contents of Bickle's privileged communications, it was not the type of intentional misconduct that was patently unconstitutional. Additionally, on the record before the court, the government's failure to literally comply with a filter procedure to segregate privileged materials that were expected in paper rather than electronic format is not the type of error likely to deter future police misconduct. The government conduct in this case does not constitute the type of deliberate, reckless, or grossly negligent disregard of the Fourth Amendment that justifies the harsh sanction of exclusion. Partial suppression of

all information received from Microsoft dated prior to March 1, 2009, and all of the unread privileged materials is an adequate remedy.

To accomplish the Ninth Circuit's direction in CDT III disapproving of wholesale seizure of records, particularly where the government fails to return materials that do not fall within the scope of what the government was authorized to seize, the court will direct that the filter agent print hard copies of emails dated on or after March 1, 2009, and provide them to the case agent who shall review the documents to seize emails falling within the scope of the warrant, *i.e.* what the government was authorized to seize. The case agent shall segregate those emails falling within the scope of the warrant from those which are not, and he shall return emails the warrant did not authorize the government to seize to counsel for Bickle. The case agent shall provide counsel for the government only with those emails the search warrant authorized the government to seize.

The court will permit ATF to keep a single copy of the DVD that was marked with an evidence sticker and placed in the ATF evidence vault for chain of custody purposes. However, the court will require that government counsel place its copy of the DVD in a sealed envelope and deposit it with the clerk of the court, under seal. The court will also direct that Ms. Martinez provide her copy of the DVD in a sealed envelope and deposit it with the clerk of the court under seal, after printing hard copies of the contents of the DVD dated on or after March 1, 2009. In completing her filter review of the contents of the DVD, Ms. Martinez shall not open or access any of the emails identified on the spreadsheet containing the names of Mr. Pokorny, Ms. Walser, or Dr. Johnson. Finally, although the court will permit ATF to keep the DVD copy marked with an evidence sticker, the court will order that ATF may not open or access the DVD without further judicial authorization. The government must apply to the court for authorization to access the contents of the DVD for forensic evaluation, chain of custody, or any other purpose.

Having reviewed and considered the matter, and for the reasons stated,

IT IS ORDERED that:

1. The ATF filter agent shall print copies of all emails on the DVD provided to her dated March 1, 2009, or after, **except for the privileged emails identified and placed on her spreadsheet containing the names Pokorny, Walser and Dr. Johnson.** She shall

provide hard copies of the non-privileged emails dated March 1, 2009, or after, to Special Agent Fox who shall review them to segregate emails falling within the scope of the warrant, *i.e.,* what was authorized to be seized.

2. After segregating non-privileged emails dated on or after March 1, 2009, which the search warrant authorized the government to seize, from those falling outside the scope of the warrant, Special Agent Fox shall return hard copies of emails falling outside the scope of the warrant to Mr. Pokorny. The government shall not keep a copy of materials on the DVD falling outside the scope of the warrant that the court has required the government to return to counsel for Bickle.

3. Special Agent Fox may only provide government counsel with non-privileged emails dated on or after March 1, 2009, falling within the scope of the warrant.

4. Counsel for Bickle may apply to the court for return of any additional materials if he reasonably believes Special Agent Fox did not return hard copies of all emails falling outside the scope of the warrant.

5. ATF may keep a single copy of the DVD that was marked with an evidence sticker and placed in the ATF vault for chain of custody purposes. However, the government shall not open or access the contents of the DVD without further judicial authorization.

6. Government counsel shall place its copy of the DVD in a sealed envelope and deposit it with the clerk of the court under seal.

7. The filter agent shall provide her copy of the DVD in a sealed envelope and deposit it with the clerk of the court under seal after she has printed hard copies as directed in this order.

IT IS RECOMMENDED that The Motion to Suppress be **GRANTED IN PART** and **DENIED IN PART** as follows:

1. The Motion to Suppress should be **GRANTED** to the extent that the following evidence should suppressed:

   (a) Any information or emails sent, received, drafted or stored in polarbickle@hotmail.com before March 1, 2009; and

(b) Any emails from polarbickle@hotmail.com identified by the filter agent from header information containing the names Pokorny, Walser, or Dr. Johnson.

2. The Motion to Suppress should be **DENIED** in all other respects.

Dated this 21st day of June, 2011.

PEGGY A. LEEN
UNITED STATES MAGISTRATE JUDGE